Editorial

Hermann de Meer*, Michael Diener, Ralph Herkenhöner, Markus Kucera, Michael Niedermeier, Andreas Reisser, Guido Schryen, Michael Vetter, Thomas Waas und Emrah Yasasin

Sicherheitsherausforderungen in hochverteilten Systemen

***Hermann de Meer:** E-Mail: hermann.demeer@uni-passau.de
Michael Diener: E-Mail: michael.diener@wiwi.uni-regensburg.de
Ralph Herkenhöner: E-Mail: ralph.herkenhoener@uni-passau.de
Markus Kucera: E-Mail: markus.kucera@hs-regensburg.de
Michael Niedermeier: E-Mail: michael.niedermeier@uni-passau.de
Andreas Reisser: E-Mail: andreas.reisser@wiwi.uni-regensburg.de
Guido Schryen: E-Mail: guido.schryen@wiwi.uni-regensburg.de
Michael Vetter: E-Mail: michael.vetter@hs-regensburg.de
Thomas Waas: E-Mail: thomas.waas@hs-regensburg.de
Emrah Yasasin: E-Mail: emrah.yasasin@wiwi.uni-regensburg.de

Schon seit Langem spielen verteilte IT-Systeme eine entscheidende Rolle in der Datenverarbeitung. Infolge der zunehmenden Vernetzung durch das Internet wurde es in den letzten Jahren möglich, global erreichbare, hochverteilte Systeme zu erschaffen. Durch die rasante Entwicklung derartiger Systeme entstehen einerseits neue Anforderungen an die Performanz (z. B. Leistungsfähigkeit und Bandbreite), während andererseits die steigende Komplexität von hochverteilten Systemen deren Absicherung (z. B. Datensicherheit und Datenschutz) immer schwieriger gestaltet. Zwei hochaktuelle Beispiele für hochverteilte Systeme sind Smart Grid und Cloud Computing, die im Folgenden näher betrachtet werden.

Smart Grid – Energieinformationsnetzwerke der Zukunft

Das intelligente Elektrizitätsnetz („Smart Grid“) wird langfristig unser heutiges, starres und hierarchisches Stromnetz ablösen. Kernziele des Smart Grid sind die Integration erneuerbarer Energiequellen, eine erhöhte Versorgungssicherheit, sowie die Bereitstellung von Infrastrukturen für eMobilität unter Berücksichtigung effizienter Verfahren hinsichtlich der Energieverwendung. Zur Realisierung dieser Ziele sind mehrere Schritte notwendig. Als Basis dieser Entwicklung dient die Verflechtung des bisher isolierten Energienetzes mit modernen Kommunikationsinfrastrukturen (vgl. Berl et al. 2013). Dies erlaubt die Integration dezentraler Energieproduktions- (z. B. Photovoltaik) und Energiespeicheranlagen (z. B. Akkumulatoren im Bereich eMobilität), sowie die Verwendung von intelligenten Stromzählern („Smart Meter“) und ermöglicht damit eine neue Qualität des Energiemanagements (z. B. durch Fernwartung und -überwachung). Neben den entstehenden Chancen durch diese Entwicklung, wie beispielsweise die Erschließung neuer Märkte, Möglichkeiten für ökonomische Wertschöpfung und ökologisch nachhaltige Energieentwicklung, ergeben sich jedoch auch Herausforderungen (vgl. Bundesnetzagentur 2011). Allein die verpflichtende Installation von Smart Metern in Haushalten stellt einen massiven Eingriff in die Privatsphäre der Bewohner dar und muss deshalb im Energie- und Datenmanagement angemessen berücksichtigt werden. In anderen Bereichen treten infrastrukturelle Fragen in den Vordergrund, wie z. B. im Bereich eMobilität, bei der die Versorgung elektrisch betriebener Fahrzeuge mit Energie eine immer wichtigere Bedeutung erlangt.

Im Folgenden werden insbesondere die Sicherheitsherausforderungen in diesem Spannungsfeld zwischen dem sich wandelnden Stromnetz einerseits und den neuen mobilen Energieverbrauchern anderseits beschrieben (vgl. McDaniel et al. 2009).

Oberste Priorität hat hierbei die hohe Verfügbarkeit des Smart Grids, welche auch unter widrigen Bedingungen, z. B. in Anwesenheit von intelligenten Angreifern, durch entsprechende Widerstandsfähigkeit gewährleistet werden muss. Aufgrund der Abhängigkeit unserer modernen Gesellschaft von der Elektrizität stellt das Smart Grid eine kritische Infrastruktur dar und folglich auch ein potentielles Angriffsziel für Terroristen, verfeindete Staaten und entschlossene Einzeltäter. Das solche Angriffe eine reale Gefahr darstellen wurde durch ein 2007 bekannt gewordenes Experiment des US-amerikanischen Department of Homeland Security bewiesen, in deren Verlauf es gelang, einen Dieselgenerator einer Kraftwerksnachbildung durch einen Cyberangriff zu zerstören (vgl. Zeller 2011). Ein weniger spektakuläres, aber dennoch bedeutendes Szenario ist ein einfacher Konsument, der seinen Zähler manipuliert um Geld zu sparen. Bereits heute ist es möglich, analoge Zähler

zu manipulieren. Bei digitalen Smart Metern stehen Angreifern jedoch noch umfangreichere Manipulationsmöglichkeiten zur Verfügung – vergleichbar ist die Situation mit der Manipulation eines digitalen Kilometerzählers im Auto. Der Nachweis kriminellen Handelns erfordert darüber hinaus detaillierte Kenntnisse in digitaler Forensik – bei einem analogen Zähler reicht meist der geübte Blick des Fachmanns. Neben Cyberkriminellen und Energiedieben stellen auch Vandalen, die entweder ohne erkennbares Ziel oder aus ideologischen Gründen agieren, eine nicht zu unterschätzende Bedrohung dar. All diese Gefährdungen müssen, unter teils enormen Kostendruck, dennoch soweit wie möglich vermieden bzw. reduziert werden. Die Verschlüsselung sensibler Daten und die Authentifizierung von Netzwerkkomponenten stellen dabei nur einen Teilaspekt dar. Die sichere Datenspeicherung, sowie die Überwachung von Zugriffen sind ebenfalls von essentieller Bedeutung. Aus diesem Grund kommt der sicheren Implementierung der erforderlichen Maßnahmen eine zentrale Bedeutung zu. Sollten nach der Installation der neuen Technik gravierende Schwachstellen gefunden werden, können diese nur mit hohem Aufwand und Kosten behoben werden. Im schlimmsten Fall ist ein manuelles Update durch Servicepersonal oder der vollständige Austausch der betroffenen Komponenten notwendig. Ein Beispiel für diese Problematik ist die im April 2013 bekannt gewordene Sicherheitslücke in Vaillants ecoPower 1.0 BHKW (vgl. Stahl 2013). Neben diesen Herausforderungen im Endkundenbereich wurde in der jüngeren Vergangenheit im Zusammenhang mit SCADA-Systemen auch der Begriff „Foreverday"-Bugs geprägt (vgl. Goodin 2012). Dies bedeutet, dass sicherheitsrelevante Fehler, die nicht gepatcht werden (können), dauerhaft in dem jeweiligen System verbleiben werden. Im Schnittbereich zwischen eMobilität und Smart Grid kommen noch besondere datenschutzrechtliche Herausforderungen hinzu. So könnten anhand der verwendeten Ladesäulen und der geladenen Energiemenge umfangreiche Bewegungsprofile erstellt werden.

Darüber hinaus stellt die Datenkommunikation zwischen Ladesäule und Fahrzeug einen weiteren Angriffsvektor dar – eine angemessene Absicherung ist deshalb unerlässlich. Zum einen um die Infrastruktur gegen Angriffe von Fahrzeugen, zum andern um Fahrzeuge gegen Angriffe durch die Infrastruktur zu schützen. Im ersten Fall könnte ein Angreifer zum Beispiel die Sicherung der Ladesäule oder den Ortsnetztransformator direkt beschädigen. Ein Beispiel für den zweiten Fall wäre die gezielte Überladung des Akkumulators bis hin zur thermischen Zerstörung des Fahrzeugs. Je nach Intention und Fähigkeiten des Angreifers kann ein einzelnes Element oder eine größere Gruppe von Entitäten Ziel eines solchen Angriffes sein.

Neben den Sicherheitsanforderungen die sich aus den oben genannten Tatsachen für das Smart Grid ergeben, stellen auch die datenschutzrechtlichen Implikationen des Smart Grids eine Herausforderungen dar. Die hochgradige Vernetzung der Teilnehmer des Energienetzes und das damit verbundene stark erhöhte Datenaufkommen innerhalb des Smart Grids führen aufgrund der erhobenen Datenmenge bei den Teilnehmern (Privatpersonen wie auch Unternehmen) der Smart Grid Initiative oft zu Bedenken hinsichtlich der potentiellen Risiken im Kontext des Datenschutzes (z. B. unerlaubte Erhebung oder Weitergabe von personenbezogenen Daten). Die möglichen Konsequenzen der Erhebung und Verarbeitung von Smart Meter Daten sind vielfältig. So können beispielsweise die Verhaltensweisen von Verbrauchern anhand des Energieverbrauchs detailgenau in Echtzeit bestimmt werden. Während diese Bedrohung nur dann zutreffen ist, falls die Kommunikation zwischen Smart Metern und Energieerzeuger direkt abgehört werden kann, ist die Speicherung und spätere Analyse von Energieverbrauchsdaten deutlich wahrscheinlicher. Mögliche Folgen sind die Erstellung von Verbrauchsprofilen, die eine Klassifizierung der einzelnen Haushalte ermöglicht. Auf dieser Grundlage können personalisierte Werbeanzeigen zugestellt werden. Hier bieten entsprechende Sicherheitsmechanismen wie beispielsweise Verschlüsselungs- und Authentifizierungsverfahren Möglichkeiten, eine unerlaubte Verwendung der Daten zu verhindern (vgl. Eckert 2011). Zudem kann mit Hilfe von Datenaggregation auf temporaler oder lokaler Ebene die Datengenauigkeit auf ein Niveau verringert werden, dass die Identifikation einzelner Haushalte unmöglich macht (vgl. Berl et al. 2013).

Cloud Computing – hochverteiltes IT-Outsourcing

Eine weitere bedeutende Strömung im Kontext hochverteilter Systeme stellen Konzepte und Technologien aus dem Bereich Cloud Computing dar. Anwender können mittels cloud-basierter Lösungen unterschiedliche Ressourcen wie z. B. Rechenleistungen, Speicherkapazitäten oder spezifische Webapplikationen bedarfsgerecht in die eigene Infrastruktur integrieren. Im Allgemeinen wird zwischen Public-, Hybrid- und Privat-Clouds (vgl. Vossen et al. 2012) unterschieden. Letztere stellen ihre Dienstleistungen für einen geschlossenen Anwenderkreis zur Verfügung, wie beispielsweise Einzelanwender oder Organisationseinheiten.

Für Unternehmen ergeben sich dadurch oftmals immense Kostenvorteile, da sie nicht bzw. kaum in Bereit-

stellungs- und Hardwarekosten investieren müssen, um eine IT-Dienstleistung nutzen zu können. Des Weiteren stellt die damit verbundene Flexibilität einen enormen Wettbewerbsvorteil dar (vgl. Hill et al. 2013), da es Unternehmen nun möglich ist, Ressourcen schnell und effektiv aus der Cloud zu allokieren. Folglich lassen sich sehr einfach auch externe Partner in spezifische Aktivitäten innerhalb einer Wertschöpfungskette einbinden.

Jedoch sind die Vorzüge von Cloud-Lösungen auch mit einer Reihe von Risiken und Nachteilen behaftet. Beispielsweise zählt hierzu die Frage des sog. Data-Ownerships (vgl. Antonopoulos et al. 2010), bei dem nicht vollständig nachgewiesen wird, wer auf Seiten des Betreibers Zugriff auf die Daten innerhalb der Cloud hat. Hierfür gibt es bereits erste Lösungsansätze, wie beispielsweise homomorphe Verschlüsselungsverfahren (vgl. Atayero et al. 2011) oder sog. Sealed Cloud[1] – Konzepte (vgl. DuD 2013), die sicherstellen können, dass Nutzdaten innerhalb der Cloud nur bestimmten Benutzern zugänglich sind. Allerdings existieren derzeit noch keine verlässlichen Verfahren, mit deren Hilfe festgestellt werden kann, ob derartige technische Maßnahmen von Cloud-Anbietern aktiv umgesetzt und implementiert werden. Für die Nutzer von Cloud-Lösungen ist eine derartige Garantie jedoch essentiell, da die Kunden üblicherweise keinen vollständigen Einblick auf die dahinterliegende Systemarchitektur haben.

Rechtskonforme Datenverarbeitung in der Cloud

Durch die zunehmende Verlagerung von IT-Prozessen in Cloud-Umgebungen ergibt sich eine Vielzahl von sicherheitstechnischen und -rechtlichen Herausforderungen (vgl. NIST 2012). Im privatwirtschaftlichen als auch im öffentlichen Bereich stellen sich zunächst zentrale Fragen der Zulässigkeit einer Verarbeitung in der Cloud. Grundsätzlich finden auch bei Cloud Computing die Grundsätze und Vorschriften für IT-Outsourcing Anwendung. Hinzu kommen jedoch neue Herausforderungen wie beispielsweise die hochverteilte, grenzübergreifende Datenverarbeitung. Diese kann dazu führen, dass Daten außerhalb zulässiger Rechtsräume verarbeitet werden. Des Weiteren muss während der Verarbeitung in der Cloud durchgehend ein ausreichendes Schutzniveau sichergestellt werden. Dieses hängt zum einen vom gesetzgeberischen Rahmen des Landes ab, in dem die datenverarbeitenden Systeme der Cloud stehen, und zum anderen aber auch von den technischen und organisatorischen Maßnahmen des Cloud Providers und der datenverarbeitenden Rechenzentren. Nicht zuletzt besitzt die Auftragskontrolle von in die Cloud ausgelagerten IT-Prozessen besondere Anforderungen. Hier wirkt sich der Vorteil einer Cloud, die technischen Vorgänge der räumlich verteilten Verarbeitung vor dem Cloud-Kunden zu verbergen, nachhaltig aus. Für eine Auftragskontrolle ist es notwendig, nachvollziehen zu können, auf welchen Systemen und an welchen Standorten (Länder, beteiligte Unternehmen) eine Verarbeitung stattgefunden hat und welche technischen und organisatorischen Maßnahmen zum Schutz der Daten wirksam angewendet wurden.

Eine zusätzliche Komplexität erlangt die oben beschriebene Situation durch die Tatsache, dass jeder Cloud-Kunde individuelle Anforderungen an Zulässigkeit, notwendigem Schutzniveau und Auftragskontrolle stellt. So ist eine Privatperson beispielsweise an dem Schutz der Privatsphäre und insbesondere der Geheimhaltung der Daten interessiert. Ein Unternehmen dagegen ist verpflichtet, neben datenschutzrechtlichen Vorgaben bzgl. Kundendaten auch finanz- und steuerrechtliche Vorgaben einzuhalten. Beispielsweise dürfen steuerrelevante Finanzdaten nur unter vorheriger Genehmigung der zuständigen Finanzbehörde außerhalb von Deutschland verarbeitet werden (vgl. § 238 HGB in Verb. m. (§ 146 Abs. 2 a AO). Nun kann es sein, dass einige Unternehmen, diese Erlaubnis erwirken konnten und andere nicht. Ein Cloud-Anbieter muss zwischen diesen Unternehmen unterscheiden können und die Daten bedarfsbezogen auf die zulässigen Verarbeitungsorte beschränken können. Auch der Nachweis einer regelkonformen Verarbeitung gegenüber Cloud-Kunden spielt eine wichtige Rolle (beispielsweise im Rahmen einer Datenverarbeitung im Auftrag gemäß §11 BDSG).

Eine weitere Hausforderung stellt der Einsatz von Sicherheitssoftware in der Cloud dar. Durch die Virtualisierung von Hardware werden CPU und Arbeitsspeicher von den Substratsystemen emuliert. Damit ist es möglich, durch Zugriff auf die Substratsysteme die virtuellen Systeme (insbesondere CPU und Arbeitsspeicher) unbemerkt auszulesen oder zu manipulieren. Für einen Cloud-Nutzer ist es somit nicht möglich festzustellen, ob ein Angreifer unerlaubt Daten aus dem Arbeitsspeicher ausliest. Bisherige Sicherheitsmaßnahmen gegen derartige Angriffe sind in der Cloud weitgehend unwirksam. Sie basieren zum einen auf Zutrittskontrollen zur physikalischen Hardware und auf Schutzmechanismen in den Betriebssystemen. Diese können bei virtuellen Systemen jedoch leichter umgangen werden, da für den Zugriff auf die Hardware eines virtuellen Systems bereits der Zugriff auf das Substratsys-

1 http://www.sealedcloud.de/, aufgerufen am 03.07.2013.

tem ausreichend ist. In einem solchen Fall ist ein Zutrittskontrollverfahren zum datenverarbeitenden System nicht mehr ausreichend und die betriebssysteminternen Maßnahmen bleiben ebenfalls unwirksam, da diese sich nur auf Prozesse innerhalb eines virtuellen Systems beziehen. Stattdessen bedarf es neuer Sicherheitsstrategien, welche direkt auf den Substratsystemen aufsetzen. Ein möglicher Lösungsansatz stellt der Einsatz sogenannter Trusted Platform Moduls (TPM) dar. Diese ermöglichen den Einsatz von hardwarebezogenen Sicherheitsmechanismen und können eine Manipulation von virtuellen Systemen wirksam verhindern (vgl. Santos 2009 und Shen 2010). Vereinfacht wird die virtuelle Hardware an die physikalische gebunden und kann nur noch bei einem direkten, physikalischen Eingriff manipuliert werden. Damit werden bewährte Maßnahmen, wie der Zutrittsschutz, wieder wirksam.

Identity Management im Kontext von Cloud Computing

Für den Betrieb von Cloud-Diensten ist ein sicheres und zuverlässiges Identity Management (IdM) unerlässlich (vgl. Fuchs et al. 2012). Dieses soll sicherstellen, dass ausschließlich berechtigte Benutzer Zugriff auf die jeweiligen Cloud-Dienste erlangen. Zudem autorisieren IdM-Komponenten die entsprechenden Anwender für bestimmte Berechtigungsobjekte. Gerade im Kontext von Cloud Computing, bei dem oftmals verschiedene Organisationseinheiten auf gemeinsame Ressourcen eines Cloud-Anbieters zugreifen, spielen IdM-Konzepte eine immer wichtigere Rolle. In diesem Zusammenhang wird häufig auch von föderierten IdM-Ansätzen (vgl. Fuchs et al. 2009) gesprochen, bei denen sich die Benutzer sicher und komfortabel bei einem zentralen Identitätsverwalter authentifizieren können. Voraussetzung für diese Form des IdM ist ein gegenseitiges Vertrauen der beteiligten Partner innerhalb der Cloud. Um eine derartige Vertrauensbasis zu schaffen, werden üblicherweise Service Level Agreements (SLAs) und Verträge verwendet, die jedoch die mit einer Cloud angestrebte Flexibilität nachhaltig einschränken können. In diesem Zusammenhang bedarf es weiterer Forschungsaktivitäten, die sich mit Konzepten beschäftigen, die eine sichere und gleichzeitig dynamische Integration von Cloud-Lösungen zulassen.

Eine weitere Problemstellung ergibt sich für Cloud-Anwender durch Lock-in-Effekte (vgl. Vossen et al. 2012). Cloud-Anbieter stellen häufig proprietäre Datenspeicherlösungen und Schnittstellen bereit, so dass eine Migration der darin gespeicherten Daten zu alternativen Cloud-Plattformen nur schwer möglich bzw. mit sehr hohen Wechselkosten verbunden ist. Die Frage nach einem Wechsel des Anbieters kann sehr schnell relevant werden, z. B. wenn ein Cloud-Anbieter nicht mehr zuverlässig seine Dienstleistung erbringt oder unverhofft in eine finanzielle Schieflage gerät. Demzufolge ist es von besonderer Relevanz, bereits vor der Auswahl eines geeigneten Cloud-Anbieters eine umfassende Evaluation durchzuführen.

Analytische Software- und Cloudsicherheit

Ein weiteres Problemfeld beschreibt den sicheren und zuverlässigen Betrieb von Software in der Cloud. Sicherheitslücken in Software- und Cloudsystemen stellen eine zunehmend große Bedrohung für die Sicherheit von Informations- und Kommunikationssystemen dar. Zur Vermeidung und Behebung dieser Sicherheitslücken werden als konkurrierende Paradigmen der Softwareentwicklung einerseits die „Closed Source-Softwareentwicklung“ und andererseits die „Open Source-Softwareentwicklung“ diskutiert. Es existiert bisher keine hinreichend breite Untersuchung zur Sicherheit der beiden Vorgehensweisen. Dem Bedarf nach weiterer Forschung auf dem Gebiet der Softwaresicherheit ist man bereits nachgekommen (vgl. Anderson 2005 und Ransbotham 2010). Eigene empirische Vorarbeiten belegen, dass die oben gestellte Frage nicht in einem konträren Diskurs beantwortet werden kann, sondern einer differenzierten Analyse der Charakteristika der beiden Entwicklungsparadigmen bedarf (vgl. Schryen 2009 und Schryen et al. 2010). Weitere Betrachtungen können dahingehen, dass neben der Untersuchung von Problematiken über die Sicherheit Open Source- vs. Closed Source-Sicherheit bei cloud-basierten Lösungen (z. B. Owncloud vs. Dropbox), auch der ökonomische Wert von Informationssystemen und die wirtschaftliche Betrachtung von Informationssysteminvestitionen mittels statistischen, spieltheoretischen sowie ökonometrischen Mitteln analysiert werden. Hier ist vor allem die Softwareentwicklung gefordert, Methoden zur Entwicklung von sicherer und zuverlässiger Software in die Entwicklungsprozesse mit einfließen zu lassen. Dies kann beispielsweise über die Bereitstellung von Entwicklungsplattformen für Cloud-Dienste erfolgen, welche das Einhalten von datenschutzrechtlichen und sicherheitstechnischen Vorgaben unterstützen. Für medizinische Anwendungen in der Cloud wurde dies bereits in einem Pilotprojekt realisiert (vgl. Fan et. al. 2011).

Überblick

In der Gesamtbetrachtung zeigt sich anhand der beiden Themengebiete Smart Grid und Cloud Computing, wie vielfältig und unterschiedlich die entstehenden Herausforderungen in Bezug auf die IT-Sicherheit sein können, die mit dem Aufkommen von hochverteilten Systemen entstehen. Dabei spielen nicht nur technische Aspekte eine Rolle, sondern auch rechtliche und ökonomische Fragestellungen, die in einem breiten interdisziplinären Rahmen zu betrachten sind. Daher ist es wichtig, Experten der verschiedenen Fachbereiche frühzeitig in einem gemeinsamen Dialog einzubinden, um praxistaugliche Sicherheitslösungen erarbeiten zu können. In den folgenden Beiträgen werden eben diese interdisziplinären Perspektiven für den Themenkomplex der hochverteilten Systeme Smart Grid und Cloud Computing dargestellt und erörtert.

Aus diesem Grund möchten wir Ihnen, liebe Leserinnen und Leser, in diesem Heft eine Zusammenstellung ausgewählter Beiträge vorstellen, welche sich mit den Sicherheitsaspekten in hochverteilten Systemen kritisch auseinandersetzen und den Themenkomplex aus rechtlicher wie auch technischer Sicht betrachten. Alle Beiträge sind im Rahmen des Symposiums „Cloud und Smart Grid – Sicherheit in verteilten Infrastrukturen“ im Rahmen der Veranstaltungsreihe „IT-Sicherheit am Donaustrand“ am 08. 02. 2013 in Passau entstanden.

Das Thema Cloud Computing leitet Herr Dr. Petri aus der Sicht des Bayerischen Landesbeauftragten für den Datenschutz in seinem Beitrag „Cloud Computing – Rechtspolitische Fragen zum Datenschutz“ ein. Er reflektiert über die datenschutzrechtliche Situation auf Landes-, Bundes- und Europaebene und veranschaulicht die Kernforderungen des Datenschutzes bei Cloud Computing. Diese greift Herr Sädtler im anschließenden Beitrag „Aktuelle Rechtsfragen des Datenschutzes und der Datensicherheit im Cloud Computing“ auf und erörtert diese aus der Sicht der aktuellen Gesetzeslage in Deutschland. Eine besondere Rolle nimmt dabei die Auftragsdatenverarbeitung ein, welche bei IT-Outsourcing häufig Anwendung findet, jedoch bei Cloud Computing vor besonderen Herausforderungen steht. Wie sicherheitstechnische Herausforderungen besser bewertet und beherrscht werden können, beschreibt Herr Perst in seinem Beitrag „Cloud-Sicherheit – wie sicher ist meine Cloud?“. Angelehnt an den BSI IT-Grundschutz stellt Herr Perst aus der Sicht eines IT-Sicherheitsexperten eine Strategie vor, welche Unternehmen in der Praxis helfen kann, den Sicherheitsbedarf im Cloud-Kontext besser bewerten zu können und somit eine Grundlage für management- und sicherheitsstrategische Entscheidungen zu bilden.

Den Smart Grid Teil eröffnet Herr Volland mit dem Beitrag „Datenschutzgerechtes Smart Metering – von den Grundrechten zum Schutzprofil“. Dieser Beitrag stellt die wesentlichen datenschutzrechtlichen Herausforderungen sowie die daran anschließenden technischen Herausforderungen dar. Insbesondere wird diskutiert, wie technische Verfahren zur Anonymisierung bzw. Pseudonymisierung zur Lösung des Konflikts zwischen den technischen Möglichkeiten bei der Datenerhebung bzw. Nutzung und den rechtlichen Vorgaben beitragen können. Vor welchen IT-sicherheitsstrategischen Herausforderungen die Praxis steht, betrachtet der anschließende Beitrag „Anforderungen an die IT-Sicherheit aus Sicht eines Verteilnetzbetreibers“ von Herrn Brantl. Dabei werden Einblicke in den technischen Betrieb der Verteilernetze gewährt und insbesondere neuartige Herausforderungen bei der Sicherstellung der Netzstabilität vorgestellt.

Der englischsprachige Beitrag „Safety & Security in Future Networks Will Need a New Internet Science” von Herrn Leopold und Herrn Bleier schließt dieses Heft ab. Er lässt sich als ein übergreifendes Fazit zu beiden Themengebieten und darüber hinaus verstehen. Er zeigt auf, vor welchen zentralen Herausforderungen wir zukünftig in hochverteilten System stehen werden und wie zu diesen geforscht und zusammengearbeitet werden kann.

Wir hoffen, dass wir Ihnen, liebe Leserinnen und Leser, mit diesen Beiträgen eine gleichermaßen hochwertige, wie auch anregende Zusammenstellung an Fachbeiträgen anbieten können und wünschen Ihnen viel Spaß beim Lesen.

Literatur

R. Anderson, Open and closed systems are equivalent (that is, in an ideal world). Perspectives on Free and Open Source Software, J. Feller, B. Fitzgerald, S. A. Hissam, K. R. Lakhani (eds), MIT Press, Cambridge, MA, Seiten 127–142, 2005.

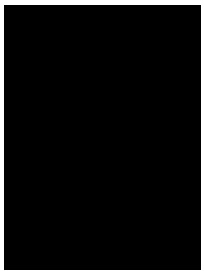
N. Antonopoulos, L. Gillam, Cloud Computing: Principles, Systems and Applications. 2010. Aufl.. Berlin, Heidelberg: Springer, 2010.

A. A. Atayero, O. Feyisetan, Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2 (10). Seiten 546–552, ISSN 2079-8407, 2011.

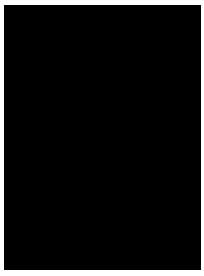
A. Berl, M. Niedermeier, H. de Meer, A. Hurson (ed.), Smart Grid Considerations – Energy Efficiency vs. Security, Green and Sustainable Computing: Part II, 88, Elsevier B.V., Seiten 159 –198, 2013.

K. V. Boesche, Leiterin der Fachgruppe Recht Begleitforschung der Förderprojekte E-Energy und IKT für Elektromobilität, Energiewirtschaftsrechtliche Anforderungen an die Implementierung von Smart Grids – Eine Einführung, EnReg Workshop Smart Grids, 2011.

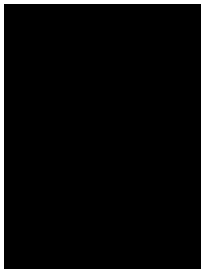
Bundesnetzagentur, „Smart Grid“ und „Smart Market“ – Eckpunktepapier der Bundesnetzagentur zu den Aspekten des sich verändernden Energieversorgungssystems, 2011.
C. Eckert, Sicherheit im Smart Grid – Eckpunkte für ein Energieinformationsnetz, Alcatel-Lucent Stiftung, 2011.
L. Fan, W. Buchanan, C. Thummler, O. Lo, A. Khedim, O. Uthmani, A. Lawson, D. Bell, Dacar platform for ehealth services cloud, In: 2011 IEEE International Conference on Cloud Computing (CLOUD), Seiten 219–226, IEEE, 2011.
L. Fuchs, G. Pernul, Minimizing insider misuse through secure Identity Management. Security and Communication Networks 5 (8), Seiten 847–862, 2012.
L. Fuchs, G. Pernul, C. Broser, Different Approaches to in-house Identity Management, In: Proc of the 4th International Conference on Availability, Reliability and Security (ARES 2009), IEEE Computer Society, Fukuoka, Japan, ISBN 978-07695-35647, 2009.
D. Goodin, Rise of “forever day” bugs in industrial systems threatens critical infrastructure, http://arstechnica.com/business/2012/04/rise-of-ics-forever-day-vulnerabiliities-threaten-critical-infrastructure/, ars technica, aufgerufen am 03.07.2013, 2012.
R. Hill, L. Hirsch, P. Lake, S. Moshiri, Guide to Cloud Computing : Principles and Practice. 2013. Aufl. ■. Berlin, Heidelberg: Springer, 2013.
P. McDaniel, S. McLaughlin, Security and Privacy Challenges in the Smart Grid, IEEE Security & Privacy, Vol. 7, Seiten 75–77, 2009.
National Institute of Standards and Technology (NIST), Cloud Computing Synopis and Recommendations, 2012.
S. Ransbotham, An Empirical Analysis of Exploitation Attempts based on Vulnerabilities in Open Source Software, in Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS), Juni, 2010.
N. Santos, K. P. Gummadi, R. Rodrigues, Towards trusted cloud computing, Proceedings of the 2009 conference on Hot topics in cloud computing, 2009.
Sealed Cloud schließt IT-Sicherheitslücke „Mensch“, In: Datenschutz und Datensicherheit – DuD 37 (5), Seite 333, 2013.
G. Schryen, Is Open-Source security a myth? What do vulnerability and patch data say?, Communications of the ACM, Vol. 54, No. 5, Seiten 130–139, 2011.
G. Schryen, E. Rich, Increasing software security through Open-Source or Closed-Source development? Empirics suggest that we have asked the wrong question, In: Proceedings of the 43rd Annual Hawaii International Conference on System Sciences (HICSS), Kauai, IEEE Computer Society, 2010.
L.-F. Stahl, Kritische Sicherheitslücke ermöglicht Fremdzugriff auf Systemregler des Vaillant ecoPOWER 1.0, http://www.bhkw-infothek.de/nachrichten/18555/2013-04-15-kritische-sicherheits lucke-ermoglicht-fremdzugriff-auf-systemregler-des-vaillant-ecopower-1-0/, aufgerufen am 03. 07. 2013, 2013.
G. Vossen, T. Haselmann, T. Hoeren, Cloud-Computing für Unternehmen: Technische, wirtschaftliche, rechtliche und organisatorische Aspekte, 1. Auflage, Heidelberg: Dpunkt.Verlag GmbH, 2012.
M. Zeller, Myth or reality – Does the Aurora vulnerability pose a risk to my generator?, 64th Annual Conference for Protective Relay Engineers 2011, Seiten 130–136, 2011.
S. Zhidong, Q. Tong, The security of cloud computing system enabled by trusted computing technology, 2010 2nd International Conference on Signal Processing Systems (ICSPS), Vol. 2, IEEE, 2010.



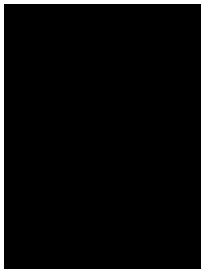
Hermann de Meer: Lehrstuhl für Rechnernetze und Rechnerkommunikation, Universität Passau, Innstrasse 43, D-94032 Passau
■■ Achtung Autor, bitte für den linken Platzhalter noch ein Porträtfoto nachlieferen ■■



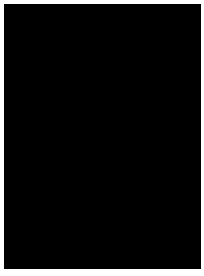
Michael Diener: Lehrstuhl Wirtschaftsinformatik I – Informationssysteme, Universität Regensburg, Universitätsstrasse 31, D-93053 Regensburg
■■ Achtung Autor, bitte für den linken Platzhalter noch ein Porträtfoto nachlieferen ■■



Ralph Herkenhöner: Lehrstuhl für Rechnernetze und Rechnerkommunikation, Universität Passau, Innstrasse 43, D-94032 Passau
■■ Achtung Autor, bitte für den linken Platzhalter noch ein Porträtfoto nachlieferen ■■

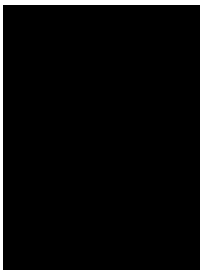


Markus Kucera: IT-Anwenderzentrum, HS-Regensburg, Universitätsstrasse 31, D-93053 Regensburg
■■ Achtung Autor, bitte für den linken Platzhalter noch ein Porträtfoto nachlieferen ■■

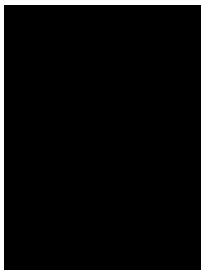


Michael Niedermeier: Lehrstuhl für Rechnernetze und Rechnerkommunikation, Universität Passau, Innstrasse 43, D-94032 Passau
■■ Achtung Autor, bitte für den linken Platzhalter noch ein Porträtfoto nachlieferen ■■

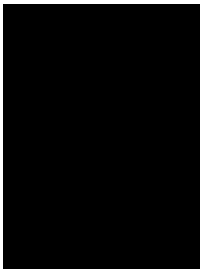
■■ Sehr geehter Herr Niedermeier, bitte liefern Sie für die schwarzen Platzhalter auf dieser und der folgenden Seite noch ein Porträtfoto für sich und die jeweiligen Co-Autoren nach, vielen Dank ■■



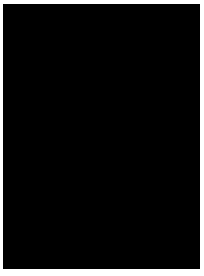
Andreas Reisser: Lehrstuhl Wirtschaftsinformatik I – Informationssysteme, Universität Regensburg, Universitätsstrasse 31, D-93053 Regensburg
■■ Achtung Autor, bitte für den linken Platzhalter noch ein Porträtfoto nachlieferen ■■



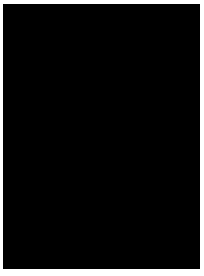
Thomas Waas: IT-Anwenderzentrum, HS-Regensburg, Universitätsstrasse 31, D-93053 Regensburg
■■ Achtung Autor, bitte für den linken Platzhalter noch ein Porträtfoto nachlieferen ■■



Guido Schryen: Professur für Wirtschaftsinformatik, Universität Regensburg, Universitätsstrasse 31, D-93053 Regensburg
■■ Achtung Autor, bitte für den linken Platzhalter noch ein Porträtfoto nachlieferen ■■



Emrah Yasasin: Professur für Wirtschaftsinformatik, Universität Regensburg, Universitätsstrasse 31, D-93053 Regensburg
■■ Achtung Autor, bitte für den linken Platzhalter noch ein Porträtfoto nachlieferen ■■



Michael Vetter: IT-Anwenderzentrum, HS-Regensburg, Universitätsstrasse 31, D-93053 Regensburg
■■ Achtung Autor, bitte für den linken Platzhalter noch ein Porträtfoto nachlieferen ■■